IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of	
Inventors: John ERICKSON et al.	: Confirmation No.: 6750
	:
U.S. Patent Application No. 09/941,606	: Group Art Unit: 2162
	:
Filed: August 30, 2001	: Examiner: Anh LY
	:
For: SOFTWARE MEDIA CONTAINER	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Attn: BOARD OF PATENT APPEALS AND INTERFERENCES

AMENDED BRIEF ON APPEAL

Further to the Notification of Non-Compliant Appeal Brief dated May 4, 2007, the Notice of Non-Compliant Appeal Brief mailed June 7, 2006, the Appeal Brief filed December 23, 2005 and the Notice of Appeal filed October 28, 2005, in connection with the above-identified application on appeal, herewith is Appellant's Amended Brief on Appeal. The $500 statutory fee was paid on December 23, 2005. The Commissioner is authorized to charge Deposit Account No. 08-2025 for any other required fees not otherwise provided for.

To the extent necessary, Appellant hereby requests any required extension of time under 37 C.F.R. §1.136 and hereby authorizes the Commissioner to charge any required fees not otherwise provided for to Deposit Account No. 08-2025.

With respect to the Notice of Non-Compliant Appeal Brief mailed June 7, 2006, Applicants assert that the Appeal Brief was compliant as claims 2 and 8 were not argued separately and therefore under 37 C.F.R. 41.37(c)(1)(v) there is no need for separate submission of these claims under the Summary of Claimed Subject Matter heading. In order to further processing of the Appeal Brief to a decision by the Board, Applicants have included additional material regarding claims 2 and 8 in the present Amended Appeal Brief.

Further, with respect to the Examiner's statement regarding media container, media handler, data external or metadata attached and media format, Applicants believe these items to have been addressed within the description of the claims in which the terms are found, e.g., media container is described with respect to at least claim 1, a media handler is not claimed but is described nonetheless with respect to at least claim 1, external data or metadata is described with respect to at least claim 1, and media format is also described with respect to at least claims 1 and 5.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

I. Real Party in Interest

The real party in interest is Hewlett-Packard Development Company, L.P., a Texas limited partnership.

II. Related Appeals and Interferences

There are no related appeals and/or interferences.

III. Status of Claims

A. Total Number of Claims in Application

1. There are a total of 11 claims in the application, which are identified as claims 1-11.

B. Status of all the claims

1. Claims canceled – None
2. Claims withdrawn from consideration but not canceled – None
3. Claims pending – 1-11
4. Claims allowed – None
5. Claims rejected – 1-11

C. Claims on Appeal

1. Claims on appeal are claims 1-11

IV. Status of Amendments

No amendments after Final Rejection have been filed.

V. Summary of Claimed Subject Matter

A media container embodiment of the claimed subject matter concerns a secure electronic media container for storing, transporting and/or providing a rights management interface to electronic media content. The secure container is "defined broadly in terms of an abstract data container format for containing data." Instant specification at page 4, lines 7-16. The secure container is provided "in the form of a universal 'envelope' or meta-container which allows for arbitrary media formats and arbitrary DRM mechanism." Instant specification at page 4, lines 25-28. In an exemplary embodiment, the container uses a "structured markup syntax such as XML, [and] has at least a <CONTENT> section and a <DRM> section." Instant specification at page 6, lines 25-27 and FIG. 2.

Electronic media content is stored in the container, e.g., an HTML file, a PDF file, an MP3 file, a Word file. Instant specification at page 6, lines 17-19. The stored electronic media content is "encrypted or otherwise arranged within the container having a notional package or 'wrapper' surrounding and protecting the stored data, such that it can only be restructured for use by a specific software program adapted especially for the format in question." Instant specification at page 4, lines 7-16 and FIG. 2. Continuing with reference to the exemplary embodiment description, the "<CONTENT> section specifies the format (e.g. the MIME type) of the content. . . . [and] can either encapsulate the content" or reference the content "by indirection through a network resource address (e.g. URL or DOI)." Instant specification at page 7, lines 1-6.

Data (also referred to as external data) representative of a media handler and/or a rights management mechanism required to open and play the electronic media content is stored external of but attached to or otherwise associated with the container. The external data is metadata attached or otherwise bound to the secure container containing media content. The metadata is "generally universally readable and/or decipherable and describe[s] the underlying media format and digital rights management mechanism(s) employed to 'package' the content." Instant specification at page 4, line 25 to page 5, line 6 and FIG. 2. A processing application "can evaluate the handling requirements of [the] container, retrieve processing components (if necessary), retrieve and render copyright ownership information, and apply designated

copyright management policies." Instant specification at page 4, line 25 to page 5, line 6. Returning again to the exemplary embodiment description, the "<DRM> section specifies the DRM mechanism employed, typically a media-specific encryption mechanism, to package the content . . . [and can] refer to either an installed component on the local system or a distant component or web service." Instant specification at page 7, lines 7-14.

As stated at page 5, lines 1-6 of the instant specification, interoperability is easier to achieve using the present claimed subject matter as "the format of the 'outer' layer of the media container . . . can be standardised, and provide a mechanism whereby a variety of digital rights management (DRM) vendors could create 'plug-in' solutions."

One or more of the foregoing advantages are achieved by the present claimed subject matter as recited in the media container of independent claim 1 which provides: A secure electronic media container for storing, transporting and/or providing a rights management interface to electronic media content, said container having said electronic media content stored therein and data, external of but attached to or otherwise associated with said container, representative of the media handler and/or a rights management mechanism required to open and play said content.

An apparatus embodiment of the claimed subject matter as claimed in claim 2 concerns an apparatus for handling the contents of a secure container as claimed in claim 1 in which is stored electronic media content of arbitrary format. The apparatus comprises means for determining from external data what, if any, digital rights management mechanism was used to package the content. The means for determining from external data the digital rights management mechanism used corresponds to at least a generic container handler 15 (FIG. 1) which "retrieves details (if any) of the DRM mechanism used to package the data within the secure container 12." Instant specification at page 5, lines 25-26. The data is attached or otherwise bound to the secure container containing media content. The data is "generally universally readable and/or decipherable and describe[s] the underlying media format and digital rights management mechanism(s) employed to 'package' the content." Instant specification at page 4, line 25 to page 5, line 6 and FIG. 2.

The means for determining further comprises retrieving or otherwise accessing an appropriate digital rights management handler accordingly. The means corresponds to at least

the generic container handler 15 of FIG. 1 described above. Further, as stated in the instant specification, "[t]he content is first passed through the specified DRM handler 14 and then through the specified media handler, such that the sound recording can now be played by the user and appropriate DRM policies can be applied accordingly." Instant specification at page 6, lines 3-6.

The apparatus comprises means for passing the content through the digital rights management handler as at least the above-described generic container handler 15 (FIG. 1). The digital rights management handler corresponds to at least DRM handler 14 (FIG. 1 and page 6, lines 1-11).

The apparatus comprises means for determining from the external data the media handler required to access and handle the content and for retrieving or otherwise accessing an appropriate media handler for passing the content through the media handler. The means corresponds to at least the generic container handler 15 of FIG. 1 described above. Further, as stated in the instant specification, "details of the media handler required to handle the data, said details being attached to the outer layer of the container 12 as metadata, together with details of how (or where) the required media handler and DRM handler can be obtained (if appropriate)." Instant specification at page 5, line 26 to page 6, line 3. Further still, the "DRM format specification (included in the metadata) indicates how the generic container (or envelope) handler 15 should recognize, reference and/or retrieve (if necessary) the required media handler(s) 16 and, in particular, how to recognise and reference particular DRM handlers or plug-ins. The DRM mechanism may be referenced in a way which is similar to the manner in which MIME types are currently handled." Instant specification at page 6, lines 7-11.

One or more of the foregoing advantages are achieved by the present claimed subject matter as recited in the media container of claim 2 which provides: An apparatus for handling the contents of a secure container as claimed in claim **1**, in which is stored electronic media content of arbitrary format, the apparatus comprising means for determining from said external data what, if any, digital rights management mechanism was used to package said content and for retrieving or otherwise accessing an appropriate digital rights management handler accordingly, means for passing said content through said digital rights management handler, means for determining from said external data the media handler required to access and handle the content and for retrieving or

otherwise accessing an appropriate media handler and means for passing said content through said media handler.

A media container embodiment of the claimed subject matter concerns a secure electronic container for storing, transporting and/or providing a rights management interface to electronic media content. As described above with respect to the media container of independent claim 1, the container has electronic media content stored therein and data, external of but attached to or otherwise associated with the container, representative of a media handler and/or a rights management mechanism required to open and play the content.

The secure container includes media content which has attached or otherwise bound thereto metadata which is universally readable and/or decipherable and describes the underlying media format and digital rights management mechanism(s) employed to package the content. As described above at page 5, second full paragraph through page 6, second paragraph, the electronic media content is stored in the container (Instant specification at page 6, lines 7-11) and is "encrypted or otherwise arranged within the container having a notional package or 'wrapper' surrounding and protecting the stored data (Instant specification at page 4, lines 7-16 and FIG. 2). The "<CONTENT> section specifies the format . . . of the content. . . . [and] can either encapsulate the content" or reference the content "by indirection through a network resource address (e.g., URL or DOI)." Instant specification at page 7, lines 1-6.

The foregoing is achieved by the present claimed subject matter as recited in the media container of dependent claim 5 which provides: A secure electronic container according to claim 3, wherein the metadata describing the underlying media format includes a remote network resource address at which the content itself is stored.

A method embodiment of the claimed subject matter concerns a method of handling the contents of a secure container as claimed in claim 1. The secure container stores electronic media content of arbitrary format as already described above with respect to claim 1. The method includes reading the external data and determining what, if any, digital rights management mechanism was used to package the content. According to an exemplary embodiment, a container handler "retrieves details (if any) of the DRM mechanism used to package the data within the secure container 12 . . ., said details being attached to the outer layer of the container 12 as metadata." Instant specification at page 5, line 22 to page 6, line 6.

The "details of how (or where) the . . . DRM handler can be obtained (if appropriate)" is specified. Instant specification at page 6, lines 2-3. The DRM details specify "how the generic container (or envelope) handler 15 should . . . recognise and reference particular DRM handlers or plug-ins."

The method further includes retrieving or otherwise accessing an appropriate digital rights management handler accordingly and passing the content through the digital rights management handler. "The content is . . . passed through the specified DRM handler 14 . . . and appropriate DRM policies can be applied accordingly." Instant specification at page 6, lines 3-6. When a container handler opens the "outer DRM envelope and determines that a DRM mechanism has been specified, [the handler] knows by the given definition of the DRM format that it must first pass the content through the specified DRM mechanism (like a filter)." Instant specification at page 7, lines 15-22 and FIG. 2.

The method further includes reading the external data and determining the media handler required to access and handle the content and retrieving or otherwise accessing the appropriate media handler and passing the content through the media handler. The metadata of the container (described above) is "readable and/or decipherable and describe[s] the underlying media format . . . so that a processing application (for example, a desktop software tool, web browser, etc.) can evaluate the handling requirements of [the] container, retrieve processing components (if necessary)." Instant specification at page 5, lines 1-6. "[D]etails of the media handler required to handle the data . . . together with details of how (or where) the required media handler . . . can be obtained" are provided in the external data. Instant specification at page 6, lines 1-6.

The present claimed subject matter provides a method of handling the contents of a secure container wherein the container stores and/or transports electronic data and includes data external of the container which is used to specify a wide range of different applications the format of the encapsulated data and provide policies on how to obtain and interpret the data content. Instant specification at page 8, lines 10-14.

One or more of the foregoing advantages are achieved by the present claimed subject matter as recited in the method of independent claim 8 which provides: A method of handling

the contents of a secure container as claimed in claim 1 in which is stored electronic media content of arbitrary format, the method comprising the steps of reading the external data and determining what, if any, digital rights management mechanism was used to package said content, retrieving or otherwise accessing an appropriate digital rights management handler accordingly, passing said content through said digital rights management handler, reading the external data and determining the media handler required to access and handle the contents, retrieving or otherwise accessing an appropriate media handler, and passing said content through said media handler.

A method embodiment of the claimed subject matter concerns a method of handling the contents of a secure container as claimed in claim 1. The secure container stores electronic media content of arbitrary format as already described above with respect to claim 1. The method includes reading the external data and determining what, if any, digital rights management mechanism was used to package the content. According to an exemplary embodiment, a container handler "retrieves details (if any) of the DRM mechanism used to package the data within the secure container 12 . . ., said details being attached to the outer layer of the container 12 as metadata." Instant specification at page 5, line 22 to page 6, line 6. The "details of how (or where) the . . . DRM handler can be obtained (if appropriate)" is specified. Instant specification at page 6, lines 2-3. The DRM details specify "how the generic container (or envelope) handler 15 should . . . recognise and reference particular DRM handlers or plug-ins."

The method further includes retrieving or otherwise accessing an appropriate digital rights management handler accordingly and passing the content through the digital rights management handler. "The content is . . . passed through the specified DRM handler 14 . . . and appropriate DRM policies can be applied accordingly." Instant specification at page 6, lines 3-6. When a container handler opens the "outer DRM envelope and determines that a DRM mechanism has been specified, [the handler] knows by the given definition of the DRM format that it must first pass the content through the specified DRM mechanism (like a filter)." Instant specification at page 7, lines 15-22 and FIG. 2.

The method further includes reading the external data and determining the media handler required to access and handle the content and retrieving or otherwise accessing the determined media handler and passing the content through the media handler. The metadata of

the container (described above) is "readable and/or decipherable and describe[s] the underlying media format . . . so that a processing application (for example, a desktop software tool, web browser, etc.) can evaluate the handling requirements of [the] container, retrieve processing components (if necessary)." Instant specification at page 5, lines 1-6. "[D]etails of the media handler required to handle the data . . . together with details of how (or where) the required media handler . . . can be obtained" are provided in the external data. Instant specification at page 6, lines 1-6.

The present claimed subject matter provides a method of handling the contents of a secure container wherein the container stores and/or transports electronic data and includes data external of the container which is used to specify a wide range of different applications the format of the encapsulated data and provide policies on how to obtain and interpret the data content. Instant specification at page 8, lines 10-14.

One or more of the foregoing advantages are achieved by the present claimed subject matter as recited in the method of independent claim 11 which provides: A method of handling the contents of a secure container as claimed in claim 1 in which is stored electronic media content of arbitrary format, the method comprising the steps of reading the external data and determining what, if any, digital rights management mechanism was used to package said content, retrieving or otherwise accessing an appropriate digital rights management handler accordingly, passing said content through said digital rights management handler, reading the external data and determining the media handler required to access and handle the contents, retrieving or otherwise accessing the determined media handler, and passing said content through said media handler.

An apparatus embodiment of the claimed subject matter concerns an apparatus for handling the contents of a secure container as claimed in claim 1. The apparatus comprises a processor arrangement for performing steps similar to those described above with respect to claim 11.

One or more of the foregoing advantages are achieved by the present claimed subject matter as recited in the apparatus of independent claim 10 which provides: Apparatus for handling the contents of a secure container as claimed in claim **1**, in which is stored electronic media content of arbitrary format, the apparatus comprising a processor arrangement for (a)

determining from said external data what, if any, digital rights management mechanism was used to package said content and for retrieving or otherwise accessing an appropriate digital rights management handler accordingly; (b) passing said content through said digital rights management handler; and (c) determining from said external data the media handler required to access and handle the content and for retrieving or otherwise accessing an appropriate media handler.

VI. Grounds of Rejection to be Reviewed on Appeal

A. The rejection of claims 1-11 under 35 U.S.C. 102(e) as being anticipated by Pub. No.: US 2001/0042043 of *Shear et al.*

VII. Argument

A. *Shear* Does Not Anticipate Claims 1-11

Claims 1 and 9

A rejection based on 35 U.S.C. §102 requires every element of the claim to be included in the reference, either directly or inherently. Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). *Shear* fails to anticipate claim 1 as *Shear* fails to disclose a secure electronic media container having electronic media content stored therein and data external of the container and representative of the media handler and/or a rights management mechanism required to open and play the content .

First, *Shear* fails to disclose data external of the container having stored therein electronic media content where the external data is representative of the media handler and/or a rights management mechanism. As stated in Appellants prior Response filed February 14, 2005, *Shear* discusses a number of general wants or desires, such as the provision of "control, rights management and/or identification solutions for the digital realm technology . . . copy protection and encryption," without providing an enabling disclosure regarding the inclusion of data representative of the media handler and/or a rights management mechanism. Appellants requested the Examiner to identify specifically where it is believed that *Shear* discloses the

features of independent claim 1 and in response, the Examiner has selected the Abstract and paragraphs 31, 41, and 51.

In the Abstract, *Shear* describes a secure software container as protectively encapsulating various digital property content and control object information. Paragraph 31 of *Shear* describes that "rights management and/or control information . . . could also be carried along with the analog signal. That is, *Shear* places the control object information within the secure software container and not external of the container. Paragraph 51 of *Shear* describes that "[e]ncryption is useful" and "a key purpose of encryption is to require the use of a copy control and rights management system in order to ensure that only those authorized to do so . . . can indeed use the content" without an enabling disclosure thereof. The identified portions of *Shear* describe at most that rights management may be important to certain parties and to that end encryption may be used to protect content, but the passages do not disclose the secure electronic media container of the present claimed subject matter. In particular, *Shear* fails to provide an enabling disclosure of data external to the container which establishes how to navigate a rights management layer to obtain and use the content within the container in order to manifest the content to a user. For at least this reason, the rejection should be reversed.

The Examiner's reference to paragraph 41 of *Shear* is not understood as there is no disclosure therein relating to data external of a container that is representative of a media handler and/or a rights management mechanism required to open and play the content.

Further, there is no disclosure of the control object information being external to the content. As described above, *Shear* places control object information within the secure software container and not external of the container. The *Shear* Abstract and paragraphs 31, 41, and 51 notwithstanding, there is no disclosure in *Shear* of external data indicating which media handler and/or rights management mechanism is required to open and play the content.

For example, the Examiner argues that the DVD of *Shear* includes "function for copy protection and including a secure software container, media handler for handling or protecting encapsulate by cryptographic techniques." Final Official Action mailed July 28, 2005 at page 2, section 4. However, *Shear* fails to disclose data external to the secure container representative of the rights management mechanism. *Shear* describes, at most, copy protection

information included in encrypted content and additional content, e.g., movie or music titles, copyright statements, audio samples, trailers, etc., stored in the clear and, importantly, within the secure container. *Shear* at paragraph 54 and "multiple sets of rules could be stored in the same 'container' on a DVD disk." at paragraph 55. Further, "a . . . secure container, together with rules about 'no copy' and/or 'copy' and/or 'numbers of permitted copies' that may apply and be enforced by consumer appliances" does not specify the rights management mechanism and instead relies on the consumer appliance being capable of determining the encoded rules and applying them to the content. *Shear* at paragraph 54. Thus, a rights management mechanism is not specified by *Shear* nor is such a mechanism specified in data external to a secure container by *Shear*.

That is, *Shear* describes copy protected content without specifying data representing a rights management mechanism required to open and play the protected content. Put another way, the *Shear*-protected content fails to include data external to the content specifying the required rights management mechanism for unprotecting the protected content. For at least this additional reason, the rejection of claim 1 should be reversed.

Claims 3, 4, 6, 7, and 9 depend, either directly or indirectly, from claim 1, include further important limitations, and are patentable over *Shear* for at least the reasons advanced above with respect to claim 1. The rejection of claims 3-7, and 9 should be reversed.

Claim 5

The reasons advanced above with respect to claim 1 are hereby incorporated by reference herein with respect to claim 5.

Claim 5 depends indirectly from claim 1, includes further important limitations, and is patentable over *Shear* for at least the reasons advanced above with respect to claim 1. For at least this reason, the rejection of claim 5 should be reversed.

Further, with specific reference to claim 5, *Shear* fails to disclose at least wherein the metadata describing the underlying media format includes a remote network resource address at which the content itself is stored. None of the Examiner-identified passages of *Shear* (page 4,

paragraph 51, page 7, paragraph 72, page 15, paragraphs 213-215, and FIGs. 7, 9, and 12) disclose a remote network resource address at which content is stored. Page 4, paragraph 51 describes that "[e]ncryption is useful" as stated above with respect to claim 1 without disclosing a remote network address as part of metadata attached or bound to a secure container containing media content. Page 7, paragraph 72 discusses a network computer being used to play a DVD wherein rights related to the DVD content may be modified by rights management capabilities provided by a remote network rights authority; however, there is no disclosure of a remote network address at which content is stored. Page 15, paragraphs 213-215 describe metadata storage of properties applicable to content without disclosing a remote network address where the content is stored. Similarly, FIGs. 7, 9, and 12 fail to provide the missing disclosure of *Shear*.

For at least this reason and for those advanced above with respect to claim 1, the rejection of claim 5 should be reversed.

Claims 2, 8, 10, and 11

The reasons advanced above with respect to claim 1 are hereby incorporated by reference herein with respect to claims 2-9 and 10-11.

Claims 2, 8 and 10-11 depend, either directly or indirectly, from claim 1, include further important limitations, and are patentable over *Shear* for at least the reasons advanced above with respect to claim 1. For at least this reason, the rejection of claims 2, 8, and 10-11 should be reversed.

Further, with specific reference to claim 11, *Shear* fails to disclose at least "reading the external data and determining the media handler required to access and handle the contents, retrieving or otherwise accessing the determined media handler, and passing said content through said media handler" according to the claimed subject matter.

The Examiner asserts that paragraphs 122-123, and 287 of *Shear* disclose determining the media handler required to access and handle the contents. Paragraphs 122 and 123 of *Shear* recite asserted benefits of the *Shear* system as including "integration into operating systems"

and "strong security." There is no disclosure of at least the step of reading the external data and determining the media handler required to access and handle the contents. *Shear* at paragraph 287, in describing multiple containers included on a DVD medium, also fails to disclose reading of the external data and determining the media handler as in the claimed subject matter. Similar to the above arguments presented regarding the rights management mechanism of the claimed subject matter of claim 1, *Shear* fails to disclose reading of data external to the container which represents the media handler required to open and play the content. *Shear* does not include the reading step as *Shear* fails to even include media handler specifying data. *Shear* does not include the media handler representative external data as the format of the content, i.e., the DVD medium, specifies the media handling mechanism to be used. Thus, there is no need for *Shear* to include external data representing a media handler.

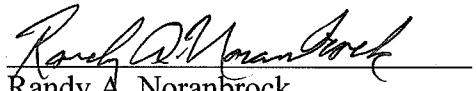
For at least this reason and for those advanced above with respect to claim 1, the rejection of claim 11 should be reversed. Claims 2, 8 and 10 are patentable over *Shear* for at least reasons similar to those advanced above with respect to claim 11.

VIII. Conclusion

Reversal of the rejection is in order.

Respectfully submitted,

John ERICKSON et al.

By: 

Randy A .Noranbrock
Reg. No. 42,940

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400
Telephone: 703-684-1111
Facsimile: 970-898-0640
Filed: **June 1, 2007**
RAN/klf/cjf

IX. Claims Appendix

1. A secure electronic media container for storing, transporting and/or providing a rights management interface to electronic media content, said container having said electronic media content stored therein and data, external of but attached to or otherwise associated with said container, representative of the media handler and/or a rights management mechanism required to open and play said content.

2. Apparatus for handling the contents of a secure container as claimed in claim **1**, in which is stored electronic media content of arbitrary format, the apparatus comprising means for determining from said external data what, if any, digital rights management mechanism was used to package said content and for retrieving or otherwise accessing an appropriate digital rights management handler accordingly, means for passing said content through said digital rights management handler, means for determining from said external data the media handler required to access and handle the content and for retrieving or otherwise accessing an appropriate media handler and means for passing said content through said media handler.

3. A secure electronic media container according to claim **1**, comprising a secure container containing media content having attached or otherwise bound thereto metadata which is universally readable and/or decipherable and describes the underlying media format and digital rights management mechanism(s) employed to package the content.

4. A secure electronic container according to claim **3**, wherein the metadata describing the underlying media format encapsulates the content itself.

5. A secure electronic container according to claim **3**, wherein the metadata describing the underlying media format includes a remote network resource address at which the content itself is stored.

6. A secure electronic container according to claim **3**, wherein said metadata includes descriptive metadata relevant to said content and/or a reference to a resource location of a format specification and/or a reference to the location of a "rendering" code registry.

7. A secure electronic container according to claim **3**, wherein said metadata describing the digital rights management mechanism(s) employed to package the content may refer to an installed component on a local system or a remote component or network service.

8. A method of handling the contents of a secure container as claimed in claim **1** in which is stored electronic media content of arbitrary format, the method comprising the steps of reading the external data and determining what, if any, digital rights management mechanism was used to package said content, retrieving or otherwise accessing an appropriate digital rights management handler accordingly, passing said content through said digital rights management handler, reading the external data and determining the media handler required to access and handle the contents, retrieving or otherwise accessing an appropriate media handler, and passing said content through said media handler.

9. A secure electronic media container according to claim **1**, wherein the data are external and attached to the container.

10. Apparatus for handling the contents of a secure container as claimed in claim **1**, in which is stored electronic media content of arbitrary format, the apparatus comprising a processor

arrangement for (a) determining from said external data what, if any, digital rights management mechanism was used to package said content and for retrieving or otherwise accessing an appropriate digital rights management handler accordingly; (b) passing said content through said digital rights management handler; and (c) determining from said external data the media handler required to access and handle the content and for retrieving or otherwise accessing an appropriate media handler.

11. A method of handling the contents of a secure container as claimed in claim 1 in which is stored electronic media content of arbitrary format, the method comprising the steps of reading the external data and determining what, if any, digital rights management mechanism was used to package said content, retrieving or otherwise accessing an appropriate digital rights management handler accordingly, passing said content through said digital rights management handler, reading the external data and determining the media handler required to access and handle the contents, retrieving or otherwise accessing the determined media handler, and passing said content through said media handler.

X. Evidence Appendix

None.

XI. Related Proceedings Appendix

None.